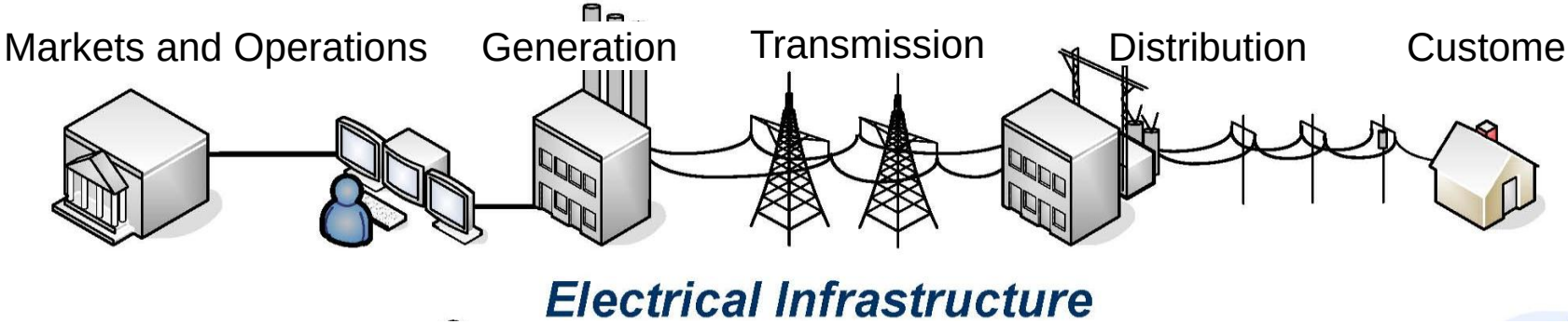
Cyber Security Working Group

Guidelines for Smart Grid Cyber Security (NISTIR 7628)

National Institute of Standards and Technology

U.S. Department of Commerce

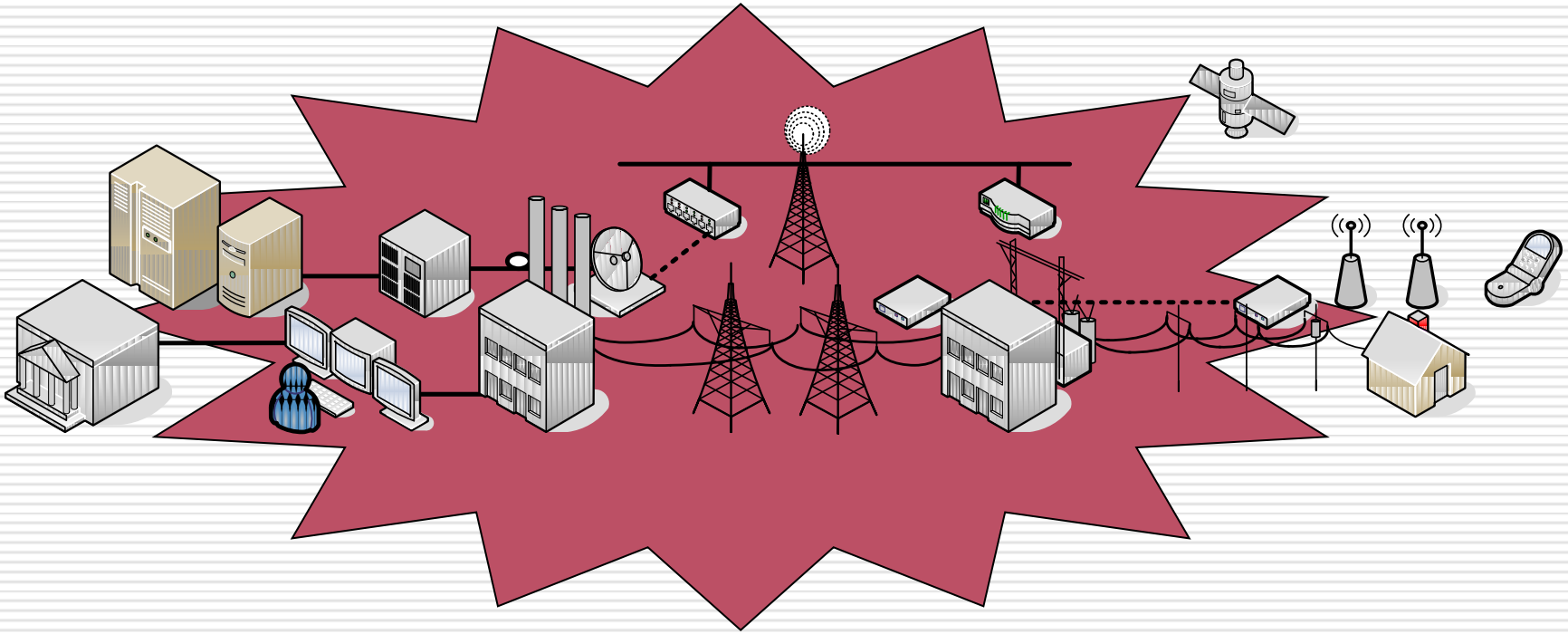
Today's Electric Grid



One-way flow of electricity

Centralized, bulk generation
Heavy reliance on coal and oil
Limited automation
Limited situational awareness
Consumers lack data to manage energy usage

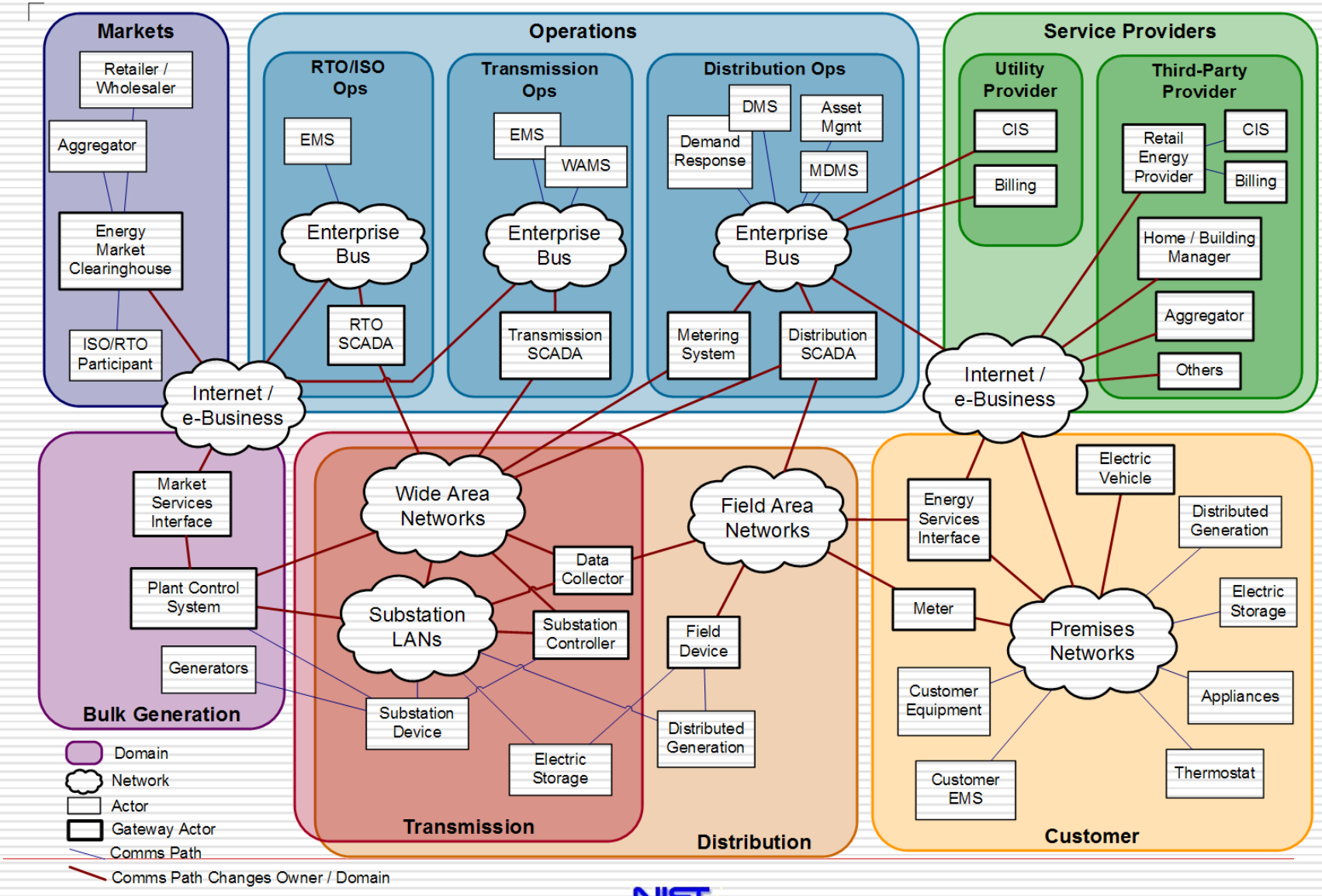
The Smart Grid



Energy Independence and Security Act

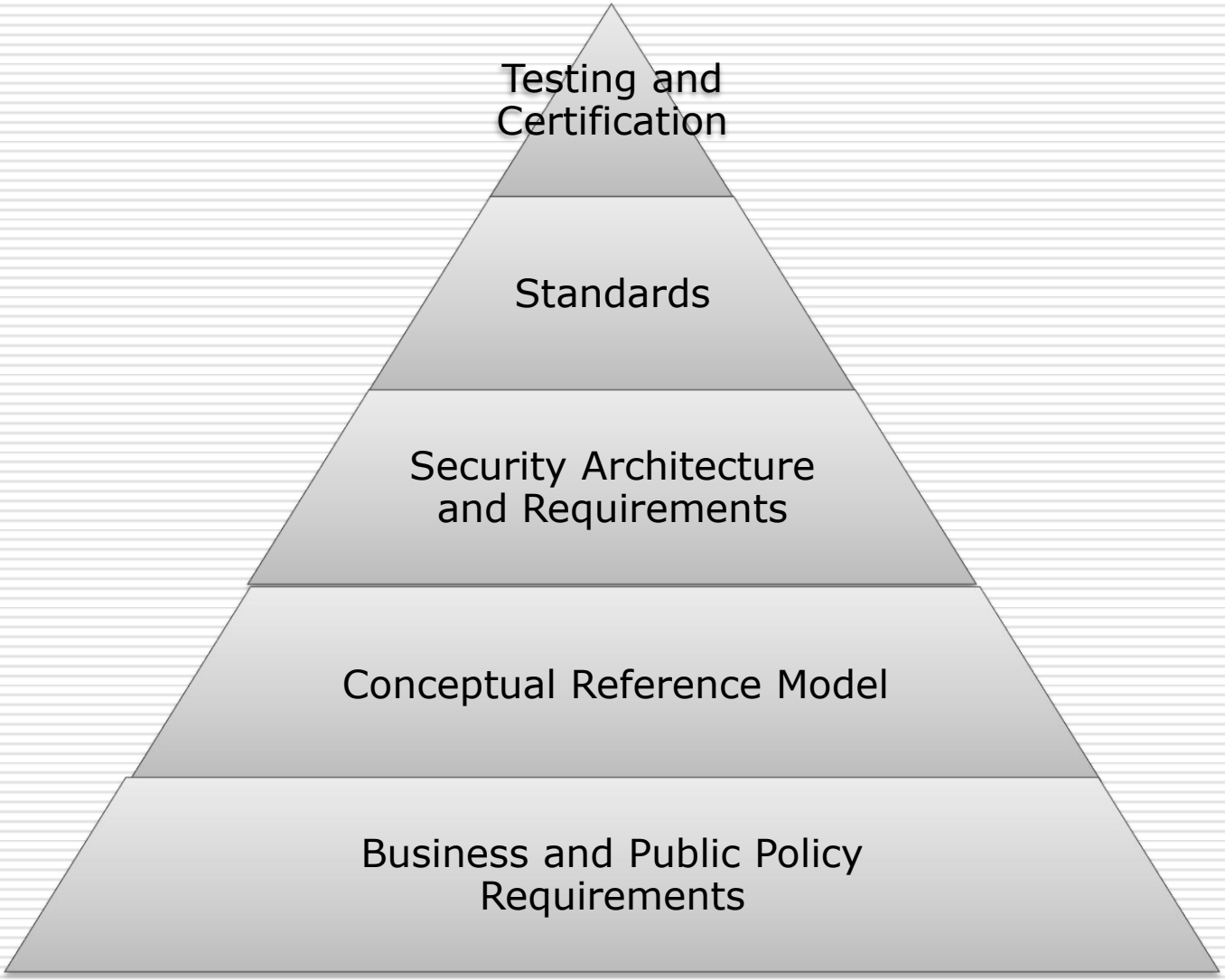
- In the Energy Independence and Security Act (EISA) of 2007, Congress established the development of a Smart Grid as a national policy goal.
- Under EISA, NIST is directed to “coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems” as well as maintain the reliability and security of the electricity infrastructure.

Conceptual Reference Diagram for Smart Grid Information Networks

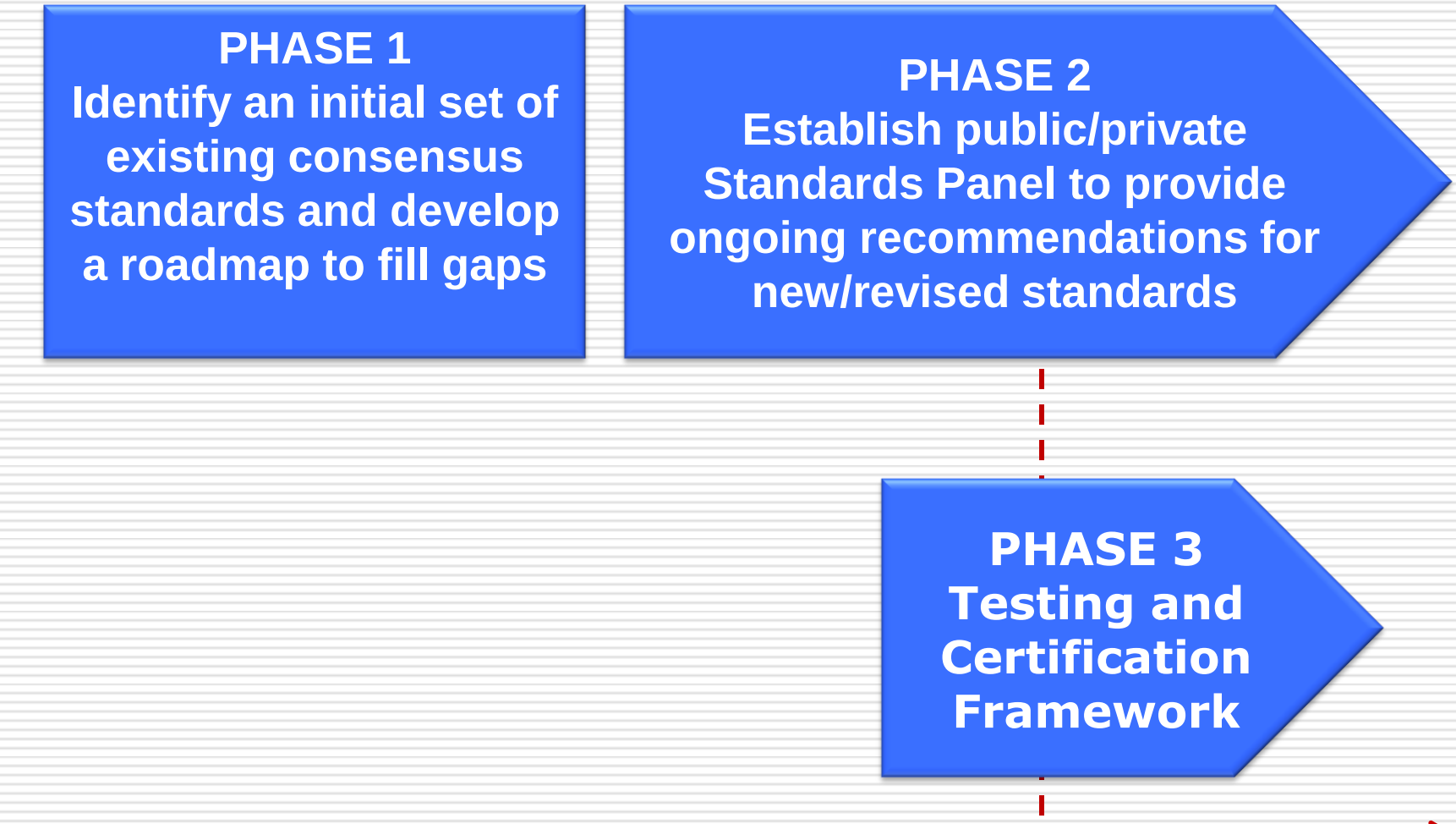


NIST
National Institute of Standards and Technology

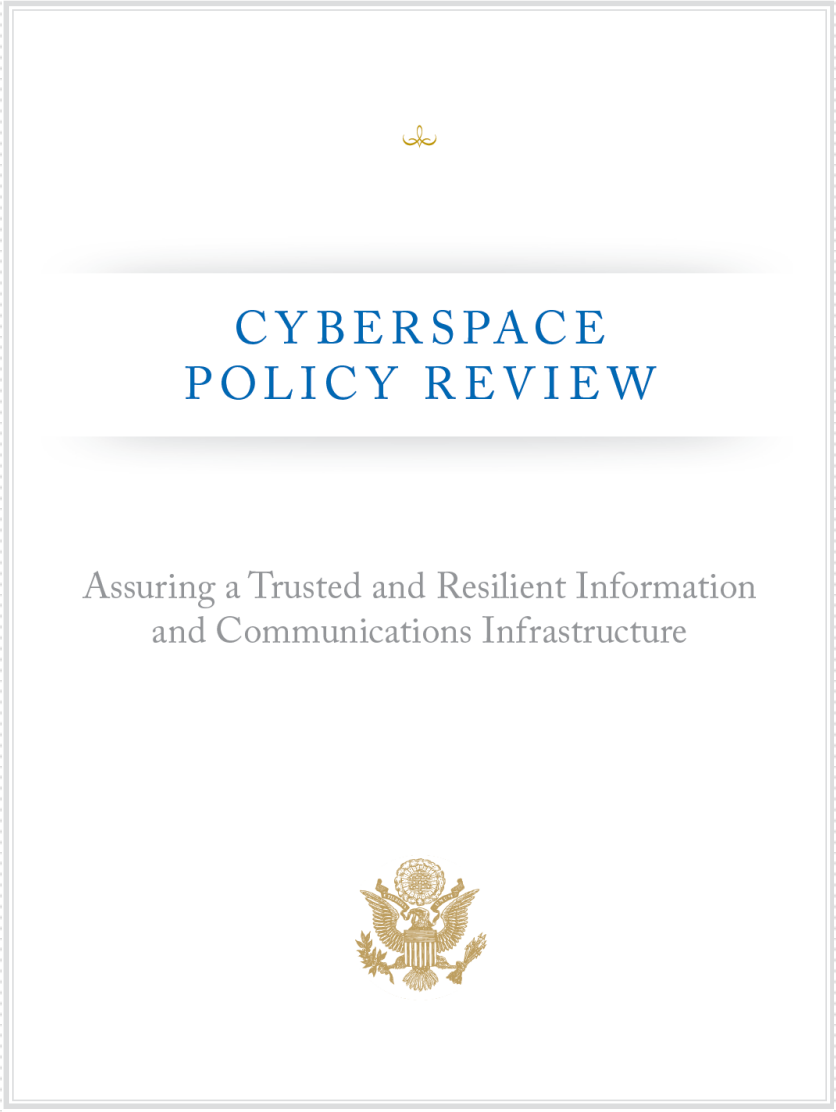
Interoperability Framework



NIST Three Phase Plan



President's Cyberspace Policy Review



…as the United States deploys new Smart Grid technology, the Federal government must ensure that security standards are developed and adopted to avoid creating unexpected opportunities for adversaries to penetrate these systems or conduct large-scale attacks.

NIST
National Institute of Standards and Technology

Smart Grid – an Opportunity

- Modernization provides an opportunity to improve security of the Grid
- Integration of new IT and networking technologies
  - Brings new risks as well as an array of security standards, processes, and tools
- Architecture is key
  - Security must be designed in – it cannot be added on later

CSWG

- To address the cross-cutting issue of cyber security, NIST established the Cyber Security Coordination Task Group (CSCTG) in March 2009.
- Moved under the NIST Smart Grid Interoperability Panel (SGIP) as a standing working group and was renamed the Cyber Security Working Group (SGIP–CSWG).

CSWG - continued

- The CSWG now has more than 500 participants from the private sector (including vendors and service providers), academia, regulatory organizations, national research laboratories, and federal agencies.

The CSWG Management Team

- Marianne Swanson – NIST Chair
- Bill Hunteman– DOE, Vice Chair
- Alan Greenberg – Boeing, Vice Chair
- Dave Dalva – CISCO, Vice Chair
- Mark Enstrom – Neustar, Secretary
- Tanya Brewer – NIST
- Victoria Yan – Booz Allen Hamilton
- Sandy Bacik - EnerNex

CSWG Meeting Info

- Weekly telecon
  - Teleconference Day & Time: Mondays, 11am Eastern Time
  - Call-in number:866-793-6322
  - Participant passcode: 3836162

CWSG Subgroups and Leads

- **Architecture Group**
  - Sandy Bacik
- **Bottom Up Group**
  - Andrew Wright; Daniel Thanos
- **Crypto and Key Management Group**
  - Daniel Thanos; Doug Biggs; Tony Metke

High Level Requirements Group

- Dave Dalva

- **Privacy Group**
  - Rebecca Herold
- **R & D Group**
  - Isaac Ghansah; Daniel Thanos
- **Standards Group**
  - Virginia Lee
- **Vulnerabilities Group**
  - Matt Carpenter, Matt Thomson
- **Security Testing and Certification Group**
  - Nelson Hastings, Sandy Bacik, and Robert Former
- **CSWG- SG AMI Security Group**
  - Darren Highfill, Ed Beroset

Guidelines for Smart Grid Cyber Security

- NIST Interagency Report 7628 - August 2010
  - Development of the document lead by NIST
  - Represents significant coordination among
    - Federal agencies
    - Private sector
    - Regulators
    - Academics
  - Document includes material that will be used in selecting and modifying security requirements

NISTIR 7628 – What it IS and IS NOT

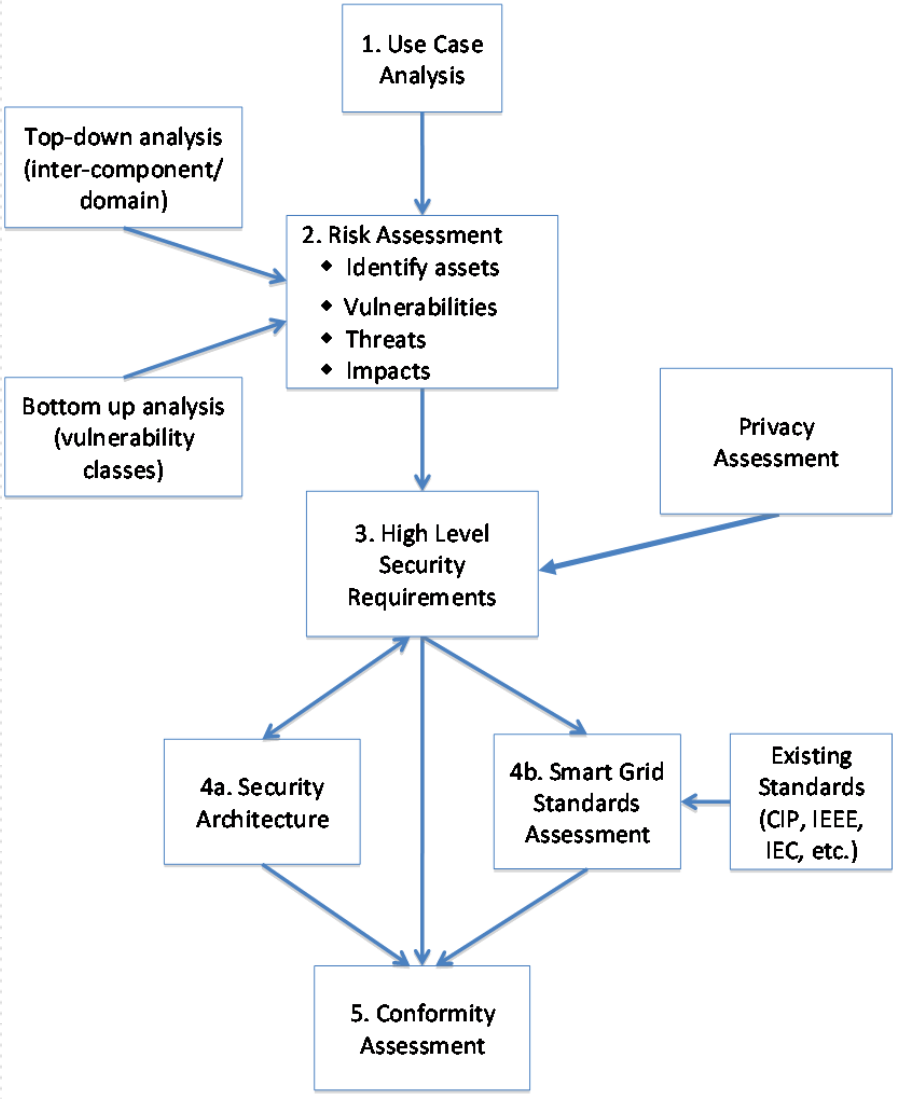
What it IS

- A tool for organizations that are researching, designing, developing, and implementing Smart Grid technologies
- May be used as a guideline to evaluate the overall cyber risks to a Smart Grid system during the design phase and during system implementation and maintenance
- Guidance for organizations
  - Each organization must develop its own cyber security strategy (including a risk assessment methodology) for the Smart Grid.

What it IS NOT

- It does not prescribe particular solutions
- It is not mandatory

Smart Grid Cyber Security Strategy - Tasks



NISTIR 7628 Content

The NISTIR includes the following

- Executive Summary
- Chapter 1 - Overall cyber security strategy for the Smart Grid
- Chapter 2 – High level and logical security architecture
- Chapter 3 – High level security requirements
- Chapter 4 – Cryptography and key management

NISTIR 7628 Content (2)

- Chapter 5 - Privacy and the Smart Grid
- Chapter 6 – Vulnerability Classes
- Chapter 7 – Bottom-up security analysis of the Smart Grid
- Chapter 8 - R&D themes for cyber security in the Smart Grid
- Chapter 9 – Overview of the standards review

NISTIR 7628 Content (3)

- Chapter 10 – Key power system use cases for security requirements
- Appendices A - J

NISTIR News

- Introduction to NISTIR 7622
  - 20 Page description of the document
  - Written for utility or security personnel
  - Describes NISTIR content
  - http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CyberSecurityCTG/Introduction_to_NISTIR_7628.pdf
- Request from Chinese Government to translate document and use within China
- Articles in many trade journals about the document

Outreach

- University of Washington - Seattle,
  - 20-21 July 2010
- Cal Poly – Pomona,
  - 10-11 August 2010
- CPUC – San Francisco,
  - 28-29 September 2010
- University of Illinois – Champaign,
  - 5 November 2010
- Georgia Tech – Atlanta,
  - 18-19 November 2010 (following NARUC meeting)

How to Participate in CSWG

- NIST Smart Grid portal
  http://nist.gov/smartgrid
- Cyber Security Working Group
  - Lead: Marianne Swanson (marianne.swanson@nist.gov)
  - NIST Support: Tanya Brewer (tanya.brewer@nist.gov)
- Cyber Security Twiki site
- http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG